CHAPTER 3

Command, Control, Communications, and Automation

Success on the battlefield depends on command, control, communications, and automation. Commanders and staff need real time communications and automation support to direct and control subordinate mission operations. Staff officers analyze data, prepare estimates, formulate plans, and supervise the execution of the commander's intent.

Success depends on communications support and the timeliness and accuracy of data provided through automated management information systems. Automation and communications systems and devices make possible real time processing and transmission of data and orders.

COMMAND AND CONTROL

Command and control are separate processes. Command provides decision and direction. Command is expressed through the commander's estimate and intent. Command charnels determine who will support and the priorities of support.

Control involves follow-up on a decision. Control is established as staff officers assess the continuous flow of information and reduce deviation from the commander's intent. Staff officers provide control by providing planning guidance and monitoring what is to be done. FM 100-5 outlines the C2 process.

GROUP COMMANDER

The group commander is responsible for C2 of the group headquarters and all assigned or attached units. The group commander aligns support provided by subordinate battalions in relation to the tactical situation and the COSCOM commander's priorities. As his second in command, the XO operates within the authority given to him by the group commander.

COMMANDER'S INTENT

The COSCOM and group commanders set forth their intent in paragraph 3 of the COSCOM/CSG OPORD. The commander's intent includes a restatement of the mission, the commander's concept of operation, and the results to be achieved. The commander uses the intent subparagraph to provide his initial guidance concerning directed, potential, and assumed missions. It

provides the basis for decentralized execution of the COSCOM/group's support missions.

The commander's intent provides staff planning guidance. It needs to be clear and concise to be understood and correctly restated one level up and two levels down. As such, it provides the basis for corps, COSCOM, and subordinate battalion commanders and staff to provide direction relative to support missions. It provides the cohesive stability during the fog of battle when C2 and communications become disrupted. It provides the common start point for staff planning. To arrive at this estimate, commanders use the nine-step planning sequence prescribed by Chapter 6 of FM 101-5.

COMMAND RELATIONSHIPS
Relationship to Subordinate Battalions

The group commander directs the relationships between group and subordinate battalion staff officers. He ensures that subordinate commanders' prerogatives for direct command are not usurped by the group's staff. Formal policy actions occur through command channels.

CSG staff officers control and coordinate the mission activities of subordinate units. They provide technical expertise and exercise technical supervision over the mission operations of subordinate units, within parameters established by the COSCOM staff. Coordination of subordinate unit activities occurs primarily through

development and implementation of SOPs, policies, and orders.

Relationship to the COSCOM

CSGs are subordinate to the COSCOM. Formal policy actions and command decisions pass through command channels. CSG staff receives policy directives and broad guidance on support functions as well as general supervision from COSCOM staff. The COSCOM staffs maintain informal liaison with the corresponding group staff on technical matters. As shown by Figure 3-1, CSG staff officers coordinate directly with their counterpart staff elements within the COSCOM HHC.

Relationship to the DISCOM

Forward CSGs coordinate reinforcing support requirements with the DISCOM and the DMMC. This includes reinforcing or augmenting support provided to FSBs and MSBs to enable them to support nondivision forces, such as corps artillery, air defense, and engineer battalions, operating in or moving through brigade and division support areas. To more effectively coordinate this support, the forward CSG commander places an LO with the DISCOM.

FM 63-2 describes the support relationship with heavy division DISCOMs. FM 63-2-1 describes the relationship with DISCOM of light infantry, airborne, and air assault divisions.

All CSG units or teams entering the division rear area report to the division rear CP. The rear CP operations cell and DISCOM CP coordinate movement routes, positions, communication links, support requirements, and security responsibilities. CSG units or teams which enter the BSA coordinate with the brigade rear CP and FSB S2/3.

To facilitate support coordination, forward CSGs develop a habitual support relationship with the division in whose area they support nondivision CS or CSS elements. The COSCOM task organizes the CSG to support requirements and work loads.

Coordination becomes imperative for support of nondivision CS and CSS forces accompanying or following a division task force or supporting offensive surge operations. This is particularly true for JP-4 or JP-8 fuel pushed forward to support corps aviation units in the division AO. Coordination is as imperative in withdrawal situations. CSG elements operating in the division AO must be kept informed of division plans. This helps prevent forward CSG units and teams getting in the way of combat troop movements along limited roads.

The limited mobility of logistics elements should not impede movement of combat elements. For this reason CSG elements with limited mobility should not employ within a band 20-35 kilometers behind the division rear boundary. During division withdrawals, these forward elements withdraw early, allowing division elements maximum freedom to maneuver.

Relationship to HostNations

To offset the shortfall of logistics units, HNS organizations may help support US forces during a crisis or war. While continuing to command and control their subordinate units, HN support commands maintain obligatory cooperation with the US supported command.

In certain theaters, cellular logistics teams provide the liaison interface between the US logistics support organization and wartime HN logistics battalions. Refer to Figure 3-2. The CMMC tasks HN logistics companies through the cellular logistics teams. These teams collocate with the HN logistics battalion. They transmit stock status reports to the CMMC.

COMMAND RELATIONSHIPS

Command relationships vary depending on whether elements are attached or placed under operational control.

Attached

The COSCOM can attach subordinate battalions or units to a CSG on a temporary basis. CSGs attach units or teams to their subordinate battalions. Based on the attachment order, the battalion commander exercises the same C2 over attached units as he does over his organic HHC.

Operational Control

To perform specific missions or tasks limited by time or location, the CSG can place units or teams under the OPCON of a subordinate battalion or unit. Elements placed under OPCON of another organization receive support from their parent organization. For example, a forward CSG could place MSTs OPCON to a division task force. The controlling commander has tactical control of the team. The MST continues to receive support from its parent unit. Note that OPCON may not include logistical, administrative, disciplinary, or training responsibilities.
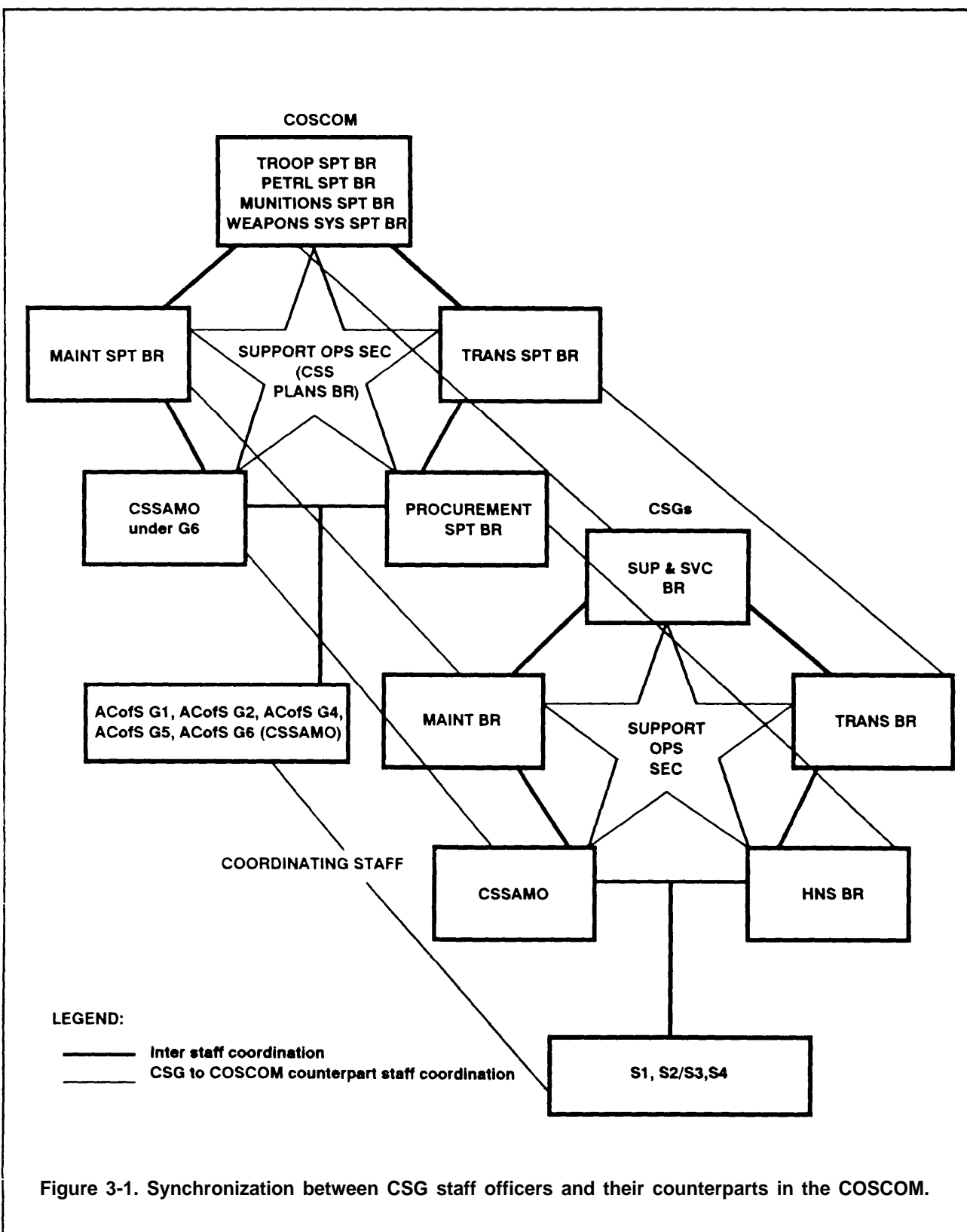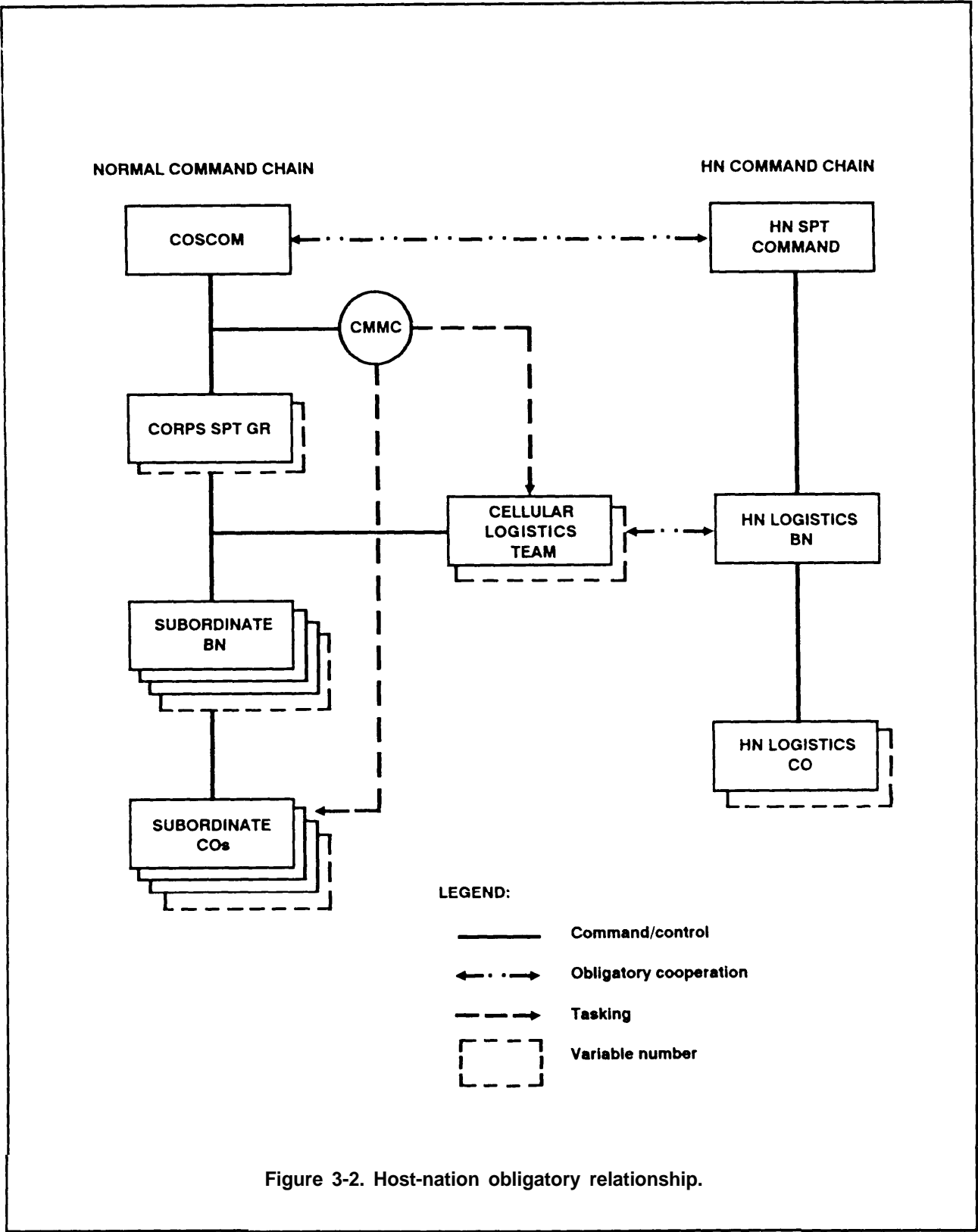
COSCOM

```
TROOP SPT BR
PETRL SPT BR
MUNITIONS SPT BR
WEAPONS SYS SPT BR
```

MAINT SPT BR

SUPPORT OPS SEC
(CSS
PLANS BR)

TRANS SPT BR

CSSAMO
under G6

PROCUREMENT
SPT BR

CSGs

SUP & SVC
BR

ACofS G1, ACofS G2, ACofS G4,
ACofS G5, ACofS G6 (CSSAMO)

MAINT BR

SUPPORT
OPS
SEC

TRANS BR

COORDINATING STAFF

CSSAMO

HNS BR

LEGEND:

——————— Inter staff coordination
_____ CSG to COSCOM counterpart staff coordination

S1, S2/S3, S4

Figure 3-1. Synchronization between CSG staff officers and their counterparts in the COSCOM.

Figure 3-2. Host-nation obligatory relationship.

COMMAND POSTS

For CSGs and subordinate battalions, CPs serve as control centers from which to plan and supervise logistics operations. CPs facilitate the acquisition, consolidation, and coordination of critical information among staff officers. Since CPs are high-value targets, FSOP reestablish CP staff from subordinate battalion staff. CPs are the first element reinforced or reestablished. OPORDs and FSOP detail the succession of command.

CSGs establish a main CP. They designate a subordinate battalion CP as their alternate CP.

MAIN COMMAND POST

The CSG main CP maintains C2 of current operations. Its logistics operations center plans support operations. It provides a facility for centralized command actions, staff coordination, and communications, The main CP –

Ž Monitors tactical operations within the CSG AO.

Ž Gathers and disseminates CSS intelligence and rear operations data.

Ž Issues OPORDs, warning orders, or fragmentary orders. (FRAGOs on previous orders save time over preparing new orders.)

Ž Maintains data on the status of resources and mission capabilities.

Ž Implements contingency plans.

CP Location

CP location depends on available cover, concealment, and access to lines of communication, It also depends on the location of the COSCOM HHC and subordinate battalion headquarters. The CSG S2/S3 selects the general location. The CSG OPORD and defense plan designates main and alternate CP locations.

To allow relatively easy access, the CP needs to be near a road network. However, for security reasons, major road junctions should be avoided. Roads need to support vehicle traffic, provide enough space to disperse vehicles, and have good drainage.

Locating the main CP in a built-up area or urban area facilitates communications and camouflage efforts. CP layout conforms to the structure of available buildings. Barns, garages, and warehouses reduce the need for extensive camouflage. Basements provide protection from enemy fires and enhance noise and light discipline. Using buildings in built-up areas reduces infrared and electromagnetic signatures. This reduces the requirement to move as often.

Staff Responsibility

The main CP operates under control of the CSG XO. Normally, CSG S2/S3 staff and communications branch personnel locate in the main CP. The S2/S3 recommends the composition and strength of security elements needed to protect the CP. The headquarters company commander establishes LPs arid OPs.

CP Displacement

The CSG main CP can be a prime threat target, especially since the sector RAOC collocates with the group headquarters. Due to its electromagnetic signature, the CSG main CP displaces as often as practicable considering the threat. The main CP may need to displace once every 8 to 17 days. The CSG HHC should maintain 75 percent mobility.

The main CP displaces in either a phased movement or a single move. The CSG S2/S3 section coordinates displacement with the sector RAOC and MCT/CMCC. It requests additional transportation assets through the supporting MCT. An advance party prepares the new site. The group S2/S3 determines the advance party composition. To speed displacement, the main CP can set up in existing urban area buildings. The XO determines the time to transfer operational control from the main CP to the new CP.

Communications need to be operatiomd during displacement. CP staffs monitor the command operations net during the move to the new CP. MSE provides MSRT users with continuous telephone service during CP displacement.

LOGISTICS OPERATIONS CENTER

The support operations section sets up a LOC to control logistics support operations. The LOC ensures that continuous logistics support is provided to support combat operations. The LOC monitors —

• DS status of supplies.

• Availability and status of service and transportation assets.

Ž Availability of weapon systems.

Ž Status of maintenance.

• External reconstitution requirements.

• Report of incidents in the CSG's sector which affect support operations.

The CSG commander or XO determines the composition of the LOC. It normally consists of support operations section staff and staff from S1 and S4 sections.

TACTICAL LOGISTICS OPERATIONS CENTER FORWARD

Key personnel from the support operations section and other sections comprise a TLOC forward. The TLOC forward moves forward to keep up with the move of the division and supported nondivision elements into forward areas. It deploys close to the division rear.

The TLOC could deploy when a division attacks or conducts turning movements. It enables the group headquarters to jump without disrupting control of CSG support operations.

ALTERNATE COMMAND POST

The alternate CP ensures continuity of C2 operations. It covers possible loss of communications with the group headquarters or destruction of the CSG main CP.

The FSOP designates which subordinate battalion headquarters operates the alternate CP. Selection depends upon the location of subordinate battalion headquarters and their organic communication capability.

If the main CP is destroyed, the surviving staff moves to the alternate CP to reconstitute the main CP. The group commander determines the time when operational control transfers from the main CP to the alternate CP. Personnel and equipment assets needed to reconstitute the main CP are drawn from subordinate battalions and units.

AUTOMATION SUPPORT

Staff officers need accurate and timely information to make estimates and prepare effective plans and orders. Their decisions depend on the quality and timeliness of the data on which they base their recommendations.

STANDARD ARMY MANAGEMENT INFORMATION SYSTEMS

STAMISs to support logistics are either in transition or under development. Refer to Figure 3-3. These systems will impact on how CSG units accomplish their missions. More detailed coverage of SAMs, SARSS, SAAS, and DAMMS-R appears in the support chapters which follow. Fielding of software systems depends on TACCS or ACCS common hardware device procurement and distribution schedules.

TACTICAL ARMY CSS COMPUTER SYSTEM

TACCS is the prototype of the small microcomputer tactical hardware required to process computer software programs. Its data entry device edits and automatically formats input. This precludes high error rates and reduces verification time.

The current automation plan calls for TACCS computers to be allocated to the CSG S1 and S4 sections. These sections use their TACCS devices to run SIDPERS and SPBS-R programs respectively. The CSS automation management office uses TACCS hardware devices to provide CSS STAMIS support to all units located in or passing through the CSG support area.

Both the S2/3 and support operations section run CSSCS on ACCS common hardware.

STANDARD INSTALLATION PERSONNEL SYSTEM

SIDPERS provides numbers only, strength accounting data, and by-name personnel accounting information. It runs on TACCS and ULC hardware. SIDPERS automates —

Ž Assignments.

Ž Organizational recordkeeping.

Ž Personnel recordkeeping.

Ž S1 personnel operations.

Subordinate units transmit unit status reports to their supporting personnel support unit. They send information copies to the CSG S1 section to enable it to perform group personnel management functions. S1 section personnel use SIDPERS reports to coordinate group strength accounting data and replacement operations.

COMBAT SERVICE SUPPORT CONTROL SYSTEM

CSSCS provides a means to collect, analyze, and present near real time data on support functions. It integrates the CSS data bases of subordinate units and supports cross-functional decision making.

Group and subordinate battalion staff officers use CSSCS to plan and coordinate support on a timely basis. CSSCS also provides decision support aids, to include message formats and algorithms. These help CSG S2/S3
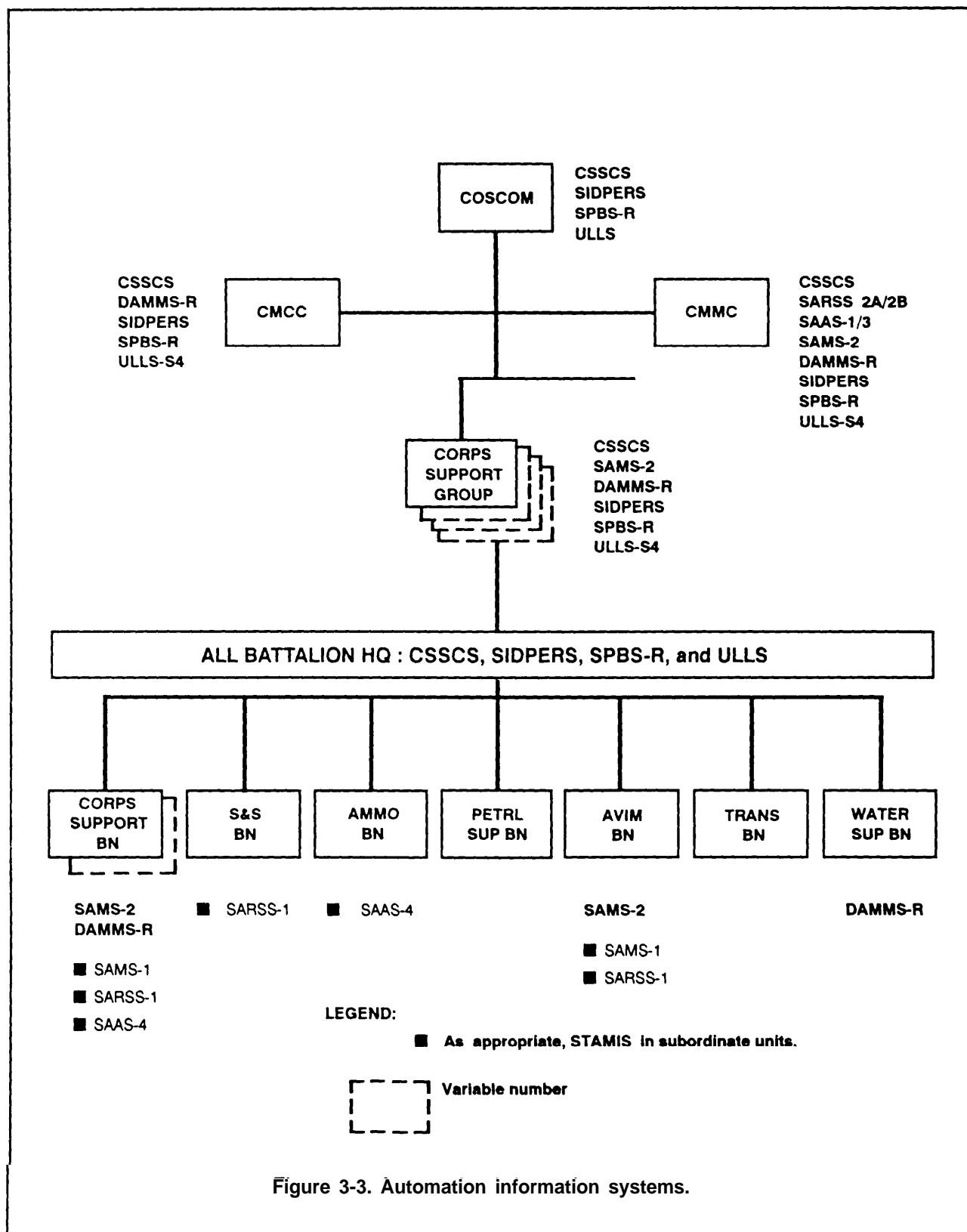
Figure 3-3. Automation information systems.

and support operations staff officers to project resource requirements and determine the supportability of alternate courses of action. They use CSSCS data to analyze and plan logistics operations. CSSCS enables CSGs to respond to emergency or special requirements from customers.

CSSCS software runs on ACCS common hardware devices. It interfaces with and retrieves data from SARSS, SAMS, SAAS, SIDPERS, and SPBS-R. CSSCS programs collect selected critical information from automated systems scheduled to support subordinate unit mission operations. Subordinate units transmit data to the CMMC.

STANDARD PROPERTY BOOK SYSTEM - REDESIGNED

SPBS-R automates property book accountability. It generates the CSG roll-up report and excess/shortage listing. It also generates CBS-X data and readiness reports.

The CSG S4 uses the asset visibility file to manage and recommend cross-leveling of assets among subordinate battalions. S4 section personnel process feeder information from subordinate battalion S4 sections. The asset visibility file maintained at the CSG S4 section can be updated with floppy disk or by telephonic interface with subordinate battalions.

UNIT-LEVEL COMPUTER

This CTA item supports company headquarters, unit supply, and unit maintenance operations. ULC interfaces with a bar code printer and LOGMARS scanner. This interface allows ULCs to read, store, write, and display soldier data tag information.

Interface between ULC, TACCS, or ACCS common hardware devices occurs through radio, wire, radio-wire integration, or commercial telephone. Electronics communication is the perferred means. Couriers with diskettes provide an alternative means of data transfer if electronics equipment is disrupted or not available.

UNIT-LEVEL LOGISTICS SYSTEM

ULLS software supports company headquarters PLL and maintenance reporting requirements. Other software programs support the materiel readiness/unit status reporting system and supply accountability procedures. ULLS allows company headquarters commanders to assess the status of equipment and thus better manage resources.

AUTOMATED SYSTEMS SECURITY

Automated systems are vulnerable to destruction, sabotage, and compromise. Security includes not only physical security of hardware devices but security of programs and procedures. Groups and subordinate battalions establish the following physical and security practices for the use of TACCS or other microcomputers:

Ž Locate the computer within an enclosure that protides controlled access.

Ž Secure all electrical facilities that support the system.

Ž Position magnetic media storage containers at least 20 inches from an exterior wall. (This helps provide protection against the potential effects of magnetic fields or radiation.)

Ž Restrict physical access to diskettes.

Ž Require that authorized operators have at least an interim confidential security clearance.

Ž Restrict access to the CSSAMO area by the use of classified passwords.

Ž Rotate unique operator passwords every 30 days or less.

Ž Control all log-ons and file access by unique operator passwords.

Ž Monitor device usage.

Ž Restrict the access of visitors.

Ž Monitor report distribution plans.

Ž Reduce the number of copies of each report.

Ž Destroy all printouts of reports and lists as new ones are printed.

CONTINUITY OF OPERATIONS

COOP plans exist at the CSG and subordinate battalions to continue operations if automated systems become inoperative due to battle loss or technical problems. One COOP safeguard requires that each computer operator dump selected system files on to a disk at the end of each day's processing. Store these disks away from the processing site.

Short-Term Outages

Outages occur due to a mechanical or power failure. During short-term outages, DS/GS unit personnel alter normal procedures as little as possible.

Long-Term Outages

When long-term outages occur, the group S4 locates replacement, substitute, or float equipment. He also arranges to time-share another command's equipment.

COMMUNICATIONS SUPPORT

The capability of communications support systems and organic communications equipment impacts the timeliness of C2 decisions. Adequate communications are required to keep up with changing tactical situations and corresponding support requirements.

MOBILE SUBSCRIBER EQUIPMENT

MSE provides a secure, mobile, survivable system capable of covering an area from the corps rear boundary to the division maneuver battalion's rear area. The system can meet the area common user voice requirements of a five division corps. It also provides area voice coverage and limited interface with adjacent corps. MSRT users can communicate over the system as long as their radio unit maintains line-of-sight contact with the radio access unit. The operational planning range is 15 kilometers from any radio access unit. The MSE network automatically bypasses and reroutes communications around damaged or jammed nodes.

Subscriber Access

Personnel enter the MSE area system via MSE compatible equipment. This includes digital telephone, radio telephone, and combat net radio. User-owned access equipment consists of –

- Digital nonsecure voice terminals.
- Mobile subscriber radio-telephone terminals.
- Facsimile equipment for informal page traffic.
- Single subscriber terminal for record traffic.

The TOE/MTOE lists MSE authorizations for CSG HHC elements.

User Responsibility

User devices such as phones, facsimiles, and MSRTs are the responsibility of the using unit. Communications branch personnel install, operate, and perform unit maintenance on subscriber terminal equipment. They also lay the wire to MSE interface points.

COMMUNICATIONS BRANCH

Personnel assigned to the communications branch operate the radio nets and the internal wire communications net. They—

- Accompany the advance party to establish the CP.
- Select the most appropriate method of transmitting messages.
- Receive, encrypt, decrypt, and transmit messages.
- Install switchboards and telephones.
- Maintain a dispatcher's map.
- Select primary and alternate messenger routes.
- Display markers for a helipad, as appropriate.
- Install light sets for the CP.
- Log in all messages.
- Install local communication wire and telephones.
- Maintain line route maps for telephone lines.
- Know and comply with COMSEC measures.

COMMUNICATIONS SECURITY

COMSEC measures deny unauthorized persons information of value. Every individual engaged in the preparation and transmission of messages, whether by telephone, radio, or messenger, need to know and follow COMSEC procedures. COMSEC measures include physical security, cryptographic security, and transmission security.

RADIO NETS

Radios supplement MSE as a means of transmitting C2 and logistics data. However, radios have limited range and retransmission capability. They are susceptible to interception, direction finding, jamming and imitative deception. Other limitations include the number of channels and length of transmission. Short, digital burst transmissions reduce electronic signature and jamming. Personnel use radios when they cannot use wire due to the distance involved. A special radio modem allows an interface with automation equipment.

Organic radios provide CSG HHC personnel access to the COSCOM command net and CSG's command operations net. They provide a means to transmit C2 information. They also transmit data if the MSE system cannot meet data transfer requirements. Table 3-1 lists VRC 12 series radios and auxiliary equipment currently authorized the base TOE. It also lists projected SINCGARS radios scheduled to replace current radios as incremental change packages are applied to the base TOE.

COSCOM Command Net (AM Radio)

CSG staff officers use the organic AM radio to communicate with their staff counterpart in the COSCOM. The AN/GRC 106 radio authorized the plans/operations branch provides long-range access to the COSCOM command net. The radio transmits information over medium to long distances (80 kilometers/50 miles) and varying terrain

Table 3-1. CSG command operations net (FM radios).

HQ ELEMENT	BASE TOE	OBJECTIVE
Command Section	AN/VRC-47 Mast AB-903/G	AN/VRC-92 (CSG Cdr) AN/VRC-90 (XO) Antenna OE-254 ( ) /GRC TSEC/KY-57

Support Ops Sec
  Trans Br
  S&S Br
  Maintenance Br
	AN/VRC-47	AN /VRC-89
		AN/VRC-90
		AN/VRC-90
		AN/VRC-90
		TSEC/KY-57 for all

S2/S3 Sec	AN/VRC-47 Antenna RC-292	AN/VRC-90 (S3) AN/VRC-92 (Signal) Antenna OE-254 ( ) /GRC TSEC/KY-57
Plans/Ops Br	AN/VRC-47 Antenna RC-292 Control Group AN/GRA-39 Power Supply	AN /VRC-90* Antenna OE-254 ( ) /GRC Control Receiver/Transmitter Power Supply TSEC/KY-57
Rear Ops Br	AN/VRC-46 Antenna RC-292 Control Group An/GRA-39 Power Supply	ANA/RC-90* Antenna OE-254 ( ) /GRC TSEC/KY-57 Control Receiver-Transmitter Power Supply
S4/S1 Sec Collocated TSEC/KY-57	ANA/RC-46	AN/VRC-90 (S4) AN/VRC-90 (S1) AN/VRC-90 (S4 Sec) Remote Terminal
Company HQ	AN/G RC-160	AN /VRC-90 TSEC/KY-57

*No OPFAC rule.

where VHF/FM is not practicable. An improved high frequency radio (AN/GRC-213) will replace the AM (AN/GRC-106) radio.

CSG Command Operations Net (FM Radio)

Organic FM radios enable CSG personnel to communicate with internal staff sections, customer units, subordinate battalions, subordinate units, base cluster units, and the sector RAOC. They provide a channel for subordinate battalions to submit status reports and customer units to resolve support problems. Table 3-1 lists VRC series 12 radios authorized in the CSG HHC base TOE. It also lists the SINCGARS radios which will replace existing radios.

SINCGARS radios provide short-range or long-range voice or digital data communications. Range varies from 8 to 35 kilometers. SINCGARS radios provide more usable channels, increased security, and increased survivability against nuclear effects and electronic countermeasures. They interface with AN/VRC-12 series radios or other FM radios operating in a single-channel mode. They also operate in a jam-resistent, frequency-hopping mode which can be changed as needed. TSEC/KY57 ensures secure voice transmission.

SIGNAL SECURITY

Jamming must be expected. CSG FSOP prescribe actions for subordinate battalions to follow upon loss of direct communications with the group headquarters.

Radio transmission can be intercepted and radio traffic analyzed. Subordinate units need to reduce the amount of logistics requirements transmitted over the command operations net. To minimize the enemy's ability to intercept and locate transmissions —

- Ž Use radios only when absolutely necessary.
- Ž Use only authorized call signs and brevity codes.
- Ž Maintain net discipline and control.
- Ž Distribute codes on a need-to-know basis.
- Ž Use authentication and encryption codes specified in the current SOI.
- Ž Keep transmission less than 20 seconds.
- Ž Use the lowest transmitter power output possible.
- Ž Avoid significant surges in radio net traffic.
- Ž Use wire and messengers whenever.

WIRE NET

A wire net provides the means for transmitting information when movement is limited and time is not available for antenna installation. Tactical secure telephones provide the primary means of communicating between the group headquarters and subordinate elements.

Current organic 2-wire TA-312 telephones and SB-22/PT switchboards cannot enter the MSE 4-wire digital system. However, even when MSE is fielded, the CSG HHC and subordinate units will retain their 2-wire telephones and switchboards to supplement internal staff communication and support rear operations security. This helps reduce the message volume sent over the MSE network.

Field telephones support internal communications, local security, perimeter defense, and LPs. Talking range depends on —

- Ž Number and quality of splices.
- Ž Weather conditions.
- Ž Number of switching centrals.
- Ž Cross-talk noise.
- Ž Other interference in a circuit.

Communications branch personnel install local phone lines within the main CP and LOC. Until fielding of MSE, the nearest area signal company runs wire to the switchboards. Following MSE fielding, wire switchboard team personnel run wire from the CP location to the MSE interface point. Signal battalion communications support teams lay wire for long distance lines.

MESSENGER SERVICE

Messenger service provides the most reliable and secure means of communicating. Couriers provide immediate delivery of high precedent traffic during periods of circuit outages or message backlogs. Using couriers eliminates the security risk associated with using radios.

Subordinate units provide their own courier service. Subordinate battalions schedule couriers to deliver daily reports on scheduled runs. Messages can be hand carried to the message center operated by the signal area support company.

HN COMMUNICATION SERVICES

If the HN has an operating telephone system, the COSCOM C-E officer may direct that the CSG use that system. Use of HN wire facilities follows the C-E annex to group plans, orders, or special instructions. The CSG C-E officer coordinates requests for HN support through the COSCOM C-E officer and corps

G5. The group and subordinate battalions maintain a phone log for each commercial phone in use.

If HN mail service is operative, units can send written communications by mail. Special instructions cover the use of HN mail service.

OPERATIONAL SECURITY

Security is a major CSS challenge. OPSEC measures deny the threat access to information. AR 530-1 describes OPSEC measures.

PHYSICAL SECURITY

CSG HHC and subordinate headquarters detachment personnel devise physical security measures to prevent espionage, sabotage, and theft and to safeguard personnel. Other physical security measures deny unauthorized access to equipment, logistics facilities, and documents. The OPSEC annex to all CSG unit FSOP describes the use of—

- Ž Random perimeter patrols.
- Ž Early warning devices.
- Ž Perimeter barriers, to include hasty mine fields.
- Ž LPs and OPs.
- Ž Sign and countersign procedures.
- Ž Access or clearance roster.
- Ž Night observation devices.

INFORMATION SECURITY

Threat forces gather information on CSG operations from something as commonplace as requisitions and shipping documents. Subordinate units need to train all personnel to deny the threat any data on the logistics status of CSG units which could reveal tactical operations of supported units.

SIGNAL SECURITY

Subordinate units train their personnel to deny the threat information from telecommunications and interception of electromagnetic radiations. SIGSEC measures include using—

- Ž Authentication procedures outlined in the CSG SOI. (Electronic notebooks provide a means of distributing the SOI.)
- Ž Call signs or call words.

- Ž Short transmissions and random transmission times.
- Ž Lowest possible radio power settings.
- Ž Correct radio antenna sitting and decoy antennas.
- Ž Alternate means of communications.

COUNTERSURVEILLANCE

All CSG units employ countersurveillance measures to prevent threat surveillance by visual, sonic, and electronic means. The OPSEC annex to all CSG unit FSOP describes the use of –

- Ž Dispersal of major items of equipment.
- Ž Smoke to screen logistics support activities.
- Ž Battlefield deception measures.
- Ž Cover, camouflage, and concealment measures.
- Ž Night resupply operations.
- Ž Noise, light, and litter discipline.
- Ž Visual shadow disrupters, to blur supply point patterns.
- Ž Traffic control procedures.

ELECTRONIC COUNTER-COUNTERMEASURES

Threat forces could attempt to gain information on CSG operations by analyzing the patterns, volume, and content of communications on the CSG command operations net. They could jam a frequency or frequency band. They could enter radio nets to deceive operators and cause confusions and delays in operations.

To prevent imitative communications deception, all communications operators need to use correct authentication procedures, call signs, and frequencies. Other measures include authorized brevity lists, prosigns, passwords, and operation codes. During any MIJI incident, operators use local command procedures to switch frequencies and send MIJI reports to the designated CEWI organization.